Configurazione di AnyConnect SSL VPN su C800v con autenticazione locale

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco IOS XE Headend C800v per una VPN SSL AnyConnect con un database utenti locale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS XE
- Cisco Secure Client (CSC)
- Operazione SSL generale
- PKI (Public Key Infrastructure)

Componenti usati

LLe informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 8000V (C800V) con versione 17.16.01a
- Cisco Secure Client versione 5.1.8.105
- PC client con Cisco Secure Client installato

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco IOS XE Secure Socket Layer (SSL) VPN è una soluzione basata su router che offre connettività VPN ad accesso remoto SSL integrata con le funzionalità di sicurezza e routing più avanzate del settore su una piattaforma convergente di dati, voce e wireless. Con la VPN SSL di Cisco IOS XE, gli utenti finali ottengono l'accesso in modo sicuro da casa o da qualsiasi postazione abilitata per Internet, ad esempio gli hotspot wireless. La VPN SSL di Cisco IOS XE consente inoltre alle aziende di estendere l'accesso alla rete aziendale a partner e consulenti offshore, mantenendo al contempo la protezione dei dati aziendali.

Questa funzionalità è supportata sulle piattaforme specificate:

Piattaforma	Versione Cisco IOS XE supportata
Cisco Cloud Services Router serie 1000V	Cisco IOS XE release 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 Integrated Services Router Cisco 4451 Integrated Services Router Cisco 4431 Integrated Services Router	Cisco IOS XE Cupertino 17.7.1a

Configurazione

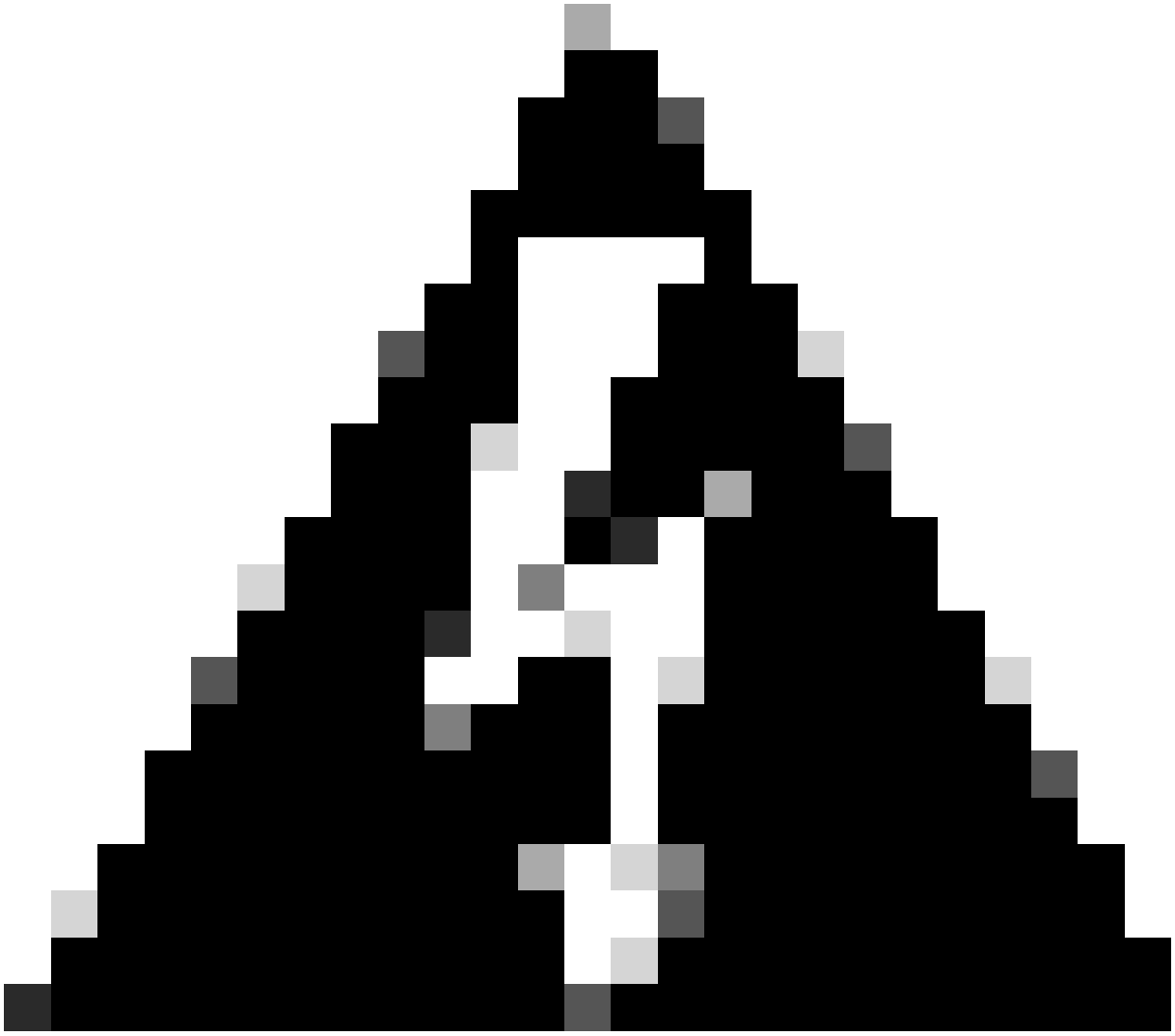
Esempio di rete

Esempio di rete di base

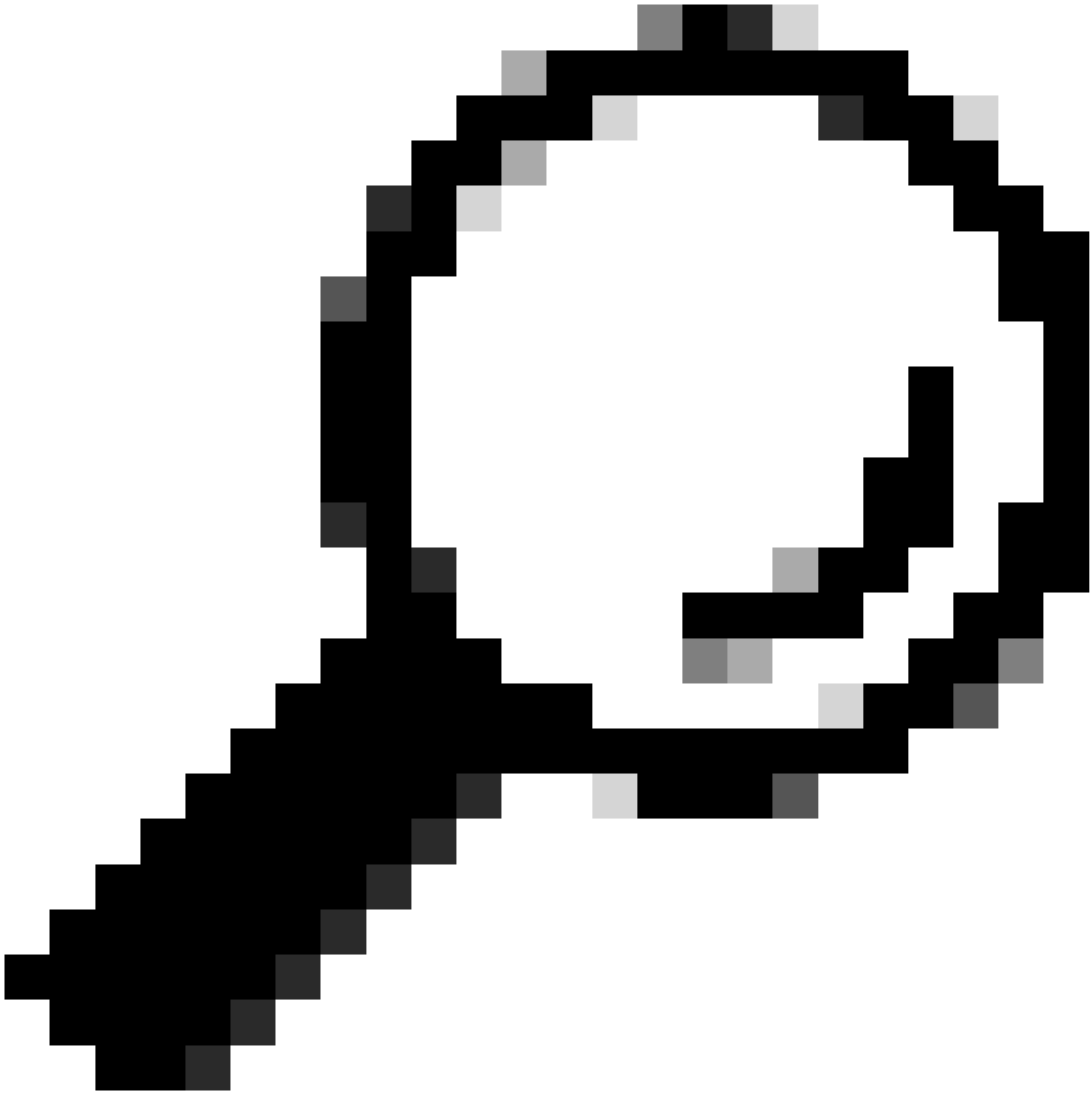
Configurazioni

1. Abilitare il server AAA, configurare l'autenticazione, gli elenchi di autorizzazioni e aggiungere un nome utente al database locale.

```
aaa new-model
!
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
!
username test password cisco123
```



Avviso: Il comando aaa new-model applica immediatamente l'autenticazione locale a tutte le righe e interfacce (ad eccezione della riga console con 0). Se si apre una sessione Telnet con il router dopo aver abilitato questo comando (o se una connessione scade e deve essere ripristinata), l'utente deve essere autenticato utilizzando il database locale del router. Si consiglia di definire un nome utente e una password sul router prima di avviare la configurazione AAA, in modo da non essere bloccati sul router.



Suggerimento: Prima di configurare i comandi AAA, salvare la configurazione. È possibile salvare nuovamente la configurazione solo dopo aver completato la configurazione AAA (e aver verificato che funzioni correttamente). Ciò consente di eseguire il ripristino in caso di blocchi imprevisti in quanto è possibile annullare qualsiasi modifica ricaricando il router.

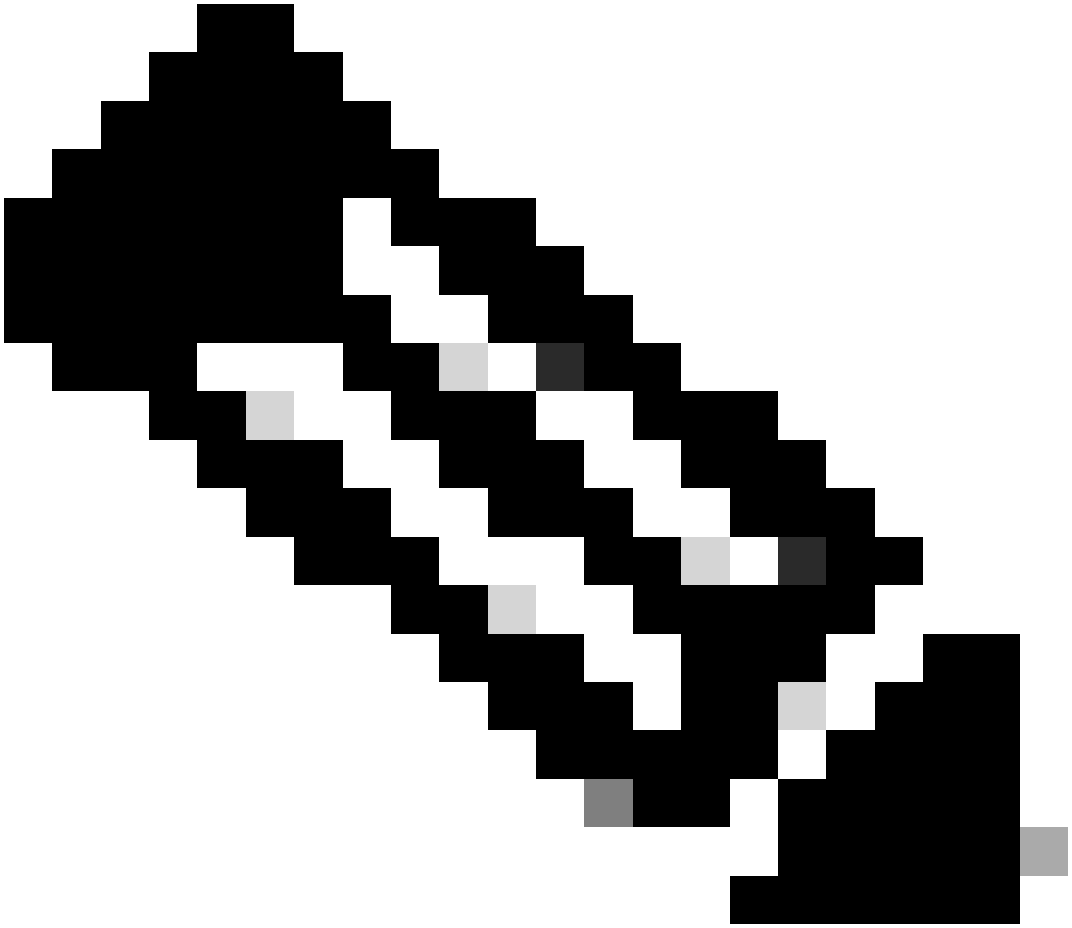
---

2. Generare Rivest-Shamir-Adleman (RSA) Keypair.

```
crypto key generate rsa label AnyConnect modulus 2048 exportable
```

3. Creare un punto di fiducia per installare il certificato di identità del router. Per ulteriori informazioni sulla creazione di certificati, vedere Configurazione della registrazione certificati per una PKI.

```
crypto pki trustpoint TP_AnyConnect
enrollment terminal
fqdn sslvpn-c8kv.example.com
subject-name cn=sslvpn-c8kv.example.com
subject-alt-name sslvpn-c8kv.example.com
revocation-check none
rsakeypair AnyConnect
```



Nota: Il nome comune (CN) nel nome soggetto deve essere configurato con l'indirizzo IP o il nome di dominio completo (FQDN) utilizzato dagli utenti per la connessione al gateway protetto (C8000V). Sebbene non sia obbligatorio, l'immissione corretta della CN consente

---

di ridurre il numero di errori di certificato riscontrati dagli utenti durante l'accesso.

4. Definire un pool locale IP per assegnare gli indirizzi a Cisco Secure Client.

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

5. (Facoltativo) Configurare un elenco degli accessi standard da utilizzare per lo split-tunnel. Questo elenco degli accessi è composto dalle reti di destinazione a cui è possibile accedere tramite il tunnel VPN. Per impostazione predefinita, tutto il traffico passa attraverso il tunnel VPN (Full Tunnel) se il tunnel suddiviso non è configurato.

```
ip access-list standard split-tunnel-acl
10 permit 192.168.11.0 0.0.0.255
20 permit 192.168.12.0 0.0.0.255
```

6.Disabilitare il server HTTP protetto.

```
no ip http secure-server
```

7. Configurare una proposta SSL.

```
crypto ssl proposal ssl_proposal
protection rsa-aes128-sha1 rsa-aes256-sha1
```

8. Configurare un criterio SSL, chiamare la proposta SSL e il trust PKI.

```
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
```

Il criterio SSL definisce la proposta e il trust point da utilizzare durante la negoziazione SSL. Funge da contenitore per tutti i parametri coinvolti nella negoziazione SSL. La selezione dei criteri viene effettuata confrontando i parametri della sessione con quelli configurati nel criterio.

9. (Facoltativo) Creare un profilo AnyConnect con l'aiuto di Cisco Secure Client Profile Editor. Cisco Secure Client Profile Editor. Viene fornito un frammento di equivalente XML del profilo per riferimento.

<#root>

```
        true

        true

        false
```

All

All

All

false

Native

true

30

false

true

false

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Disable

```
false
```

```
false
```

```
 20
```

```
 4
```

```
false
```

```
false
```

```
true
```

SSL_C8KV

sslvpn-c8kv.example.com

10. Caricare il profilo XML creato nella memoria flash del router e definire il profilo:

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

11.Disabilitare il server protetto HTTP.

```
no ip http secure-server
```

12. Configurare i criteri di autorizzazione SSL.

```
crypto ssl authorization policy ssl_author_policy
client profile acvpn
pool SSLVPN_POOL
dns 192.168.11.100
banner Welcome to C8kv SSLVPN
def-domain example.com
route set access-list split-tunnel-acl
```

Il criterio di autorizzazione SSL è un contenitore di parametri di autorizzazione sottoposti a PUSH nel client remoto.Il criterio di autorizzazione è indicato dal profilo SSL.

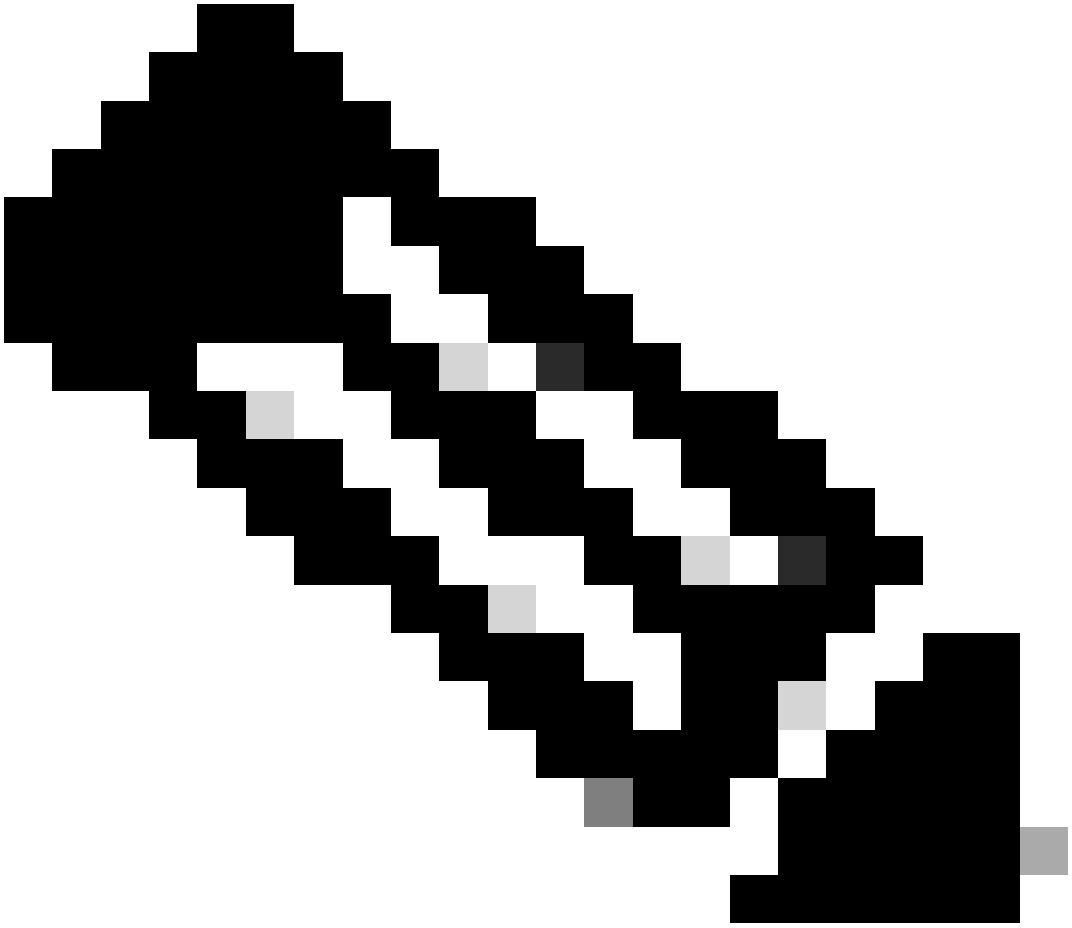
13. Configurare un modello virtuale da cui vengono clonate le interfacce di accesso virtuale.

```
interface Virtual-Template2 type vpn
ip unnumbered GigabitEthernet1
ip mtu 1400
ip tcp adjust-mss 1300
```

14. Configurare un profilo SSL e definire l'autenticazione, gli elenchi di accounting e il modello virtuale.

```
crypto ssl profile ssl_prof
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
```

La selezione di un profilo dipende dai criteri e dai valori URL.



Nota: Il criterio e l'URL devono essere univoci per un profilo VPN SSL e deve essere specificato almeno un metodo di autorizzazione per avviare la sessione.

Questi sono utilizzati nel profilo SSL:

- criterio match - istruzione match per selezionare un profilo SSL ssl_prof per un client sul nome del criterio SSL ssl_policy.
- match url - istruzioni match per selezionare un profilo SSL ssl_prof per un client nella cartella URL sslvpn-c8kv.example.com.
- aaa authentication user-pass list: durante l'autenticazione viene utilizzato l'elenco SSLVPN_AUTHEN.
- aaa authorization group user-pass list: durante l'autorizzazione, l'elenco delle reti SSLVPN_AUTHOR viene utilizzato con il criterio di autorizzazione ssl_author_policy.
- authentication remote user-pass: definisce la modalità di autenticazione del client remoto basata su nome utente/password.
- virtual-template 2: definisce il modello virtuale da clonare.

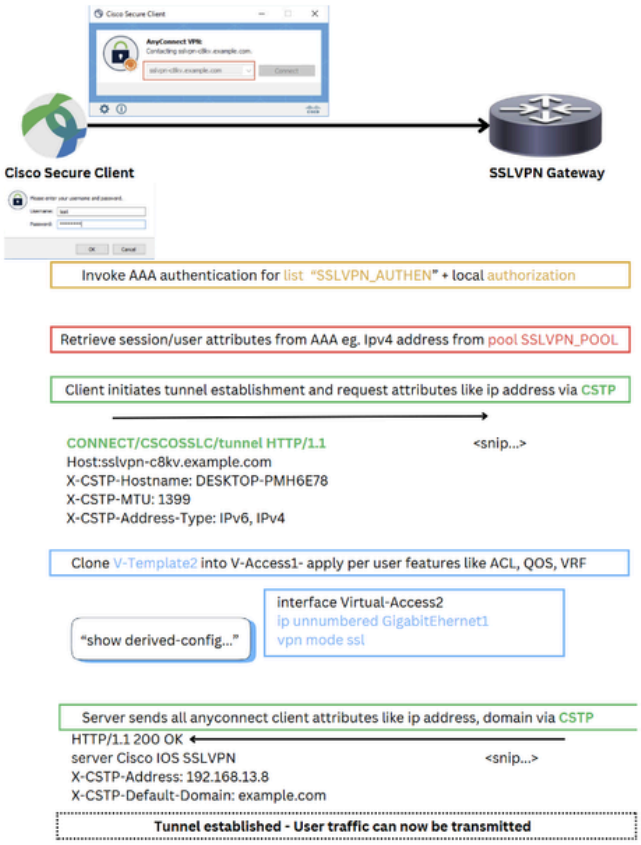
Flusso connessione

Per informazioni sugli eventi che si verificano tra Cisco Secure Client e il gateway sicuro durante la connessione VPN SSL, consultare il documento [Informazioni sul flusso della connessione VPN SSL AnyConnect]

Flusso di connessione ad alto livello da Cisco Secure Client (AnyConnect) a C800v


```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

Flusso di connessione ad alto livello 1

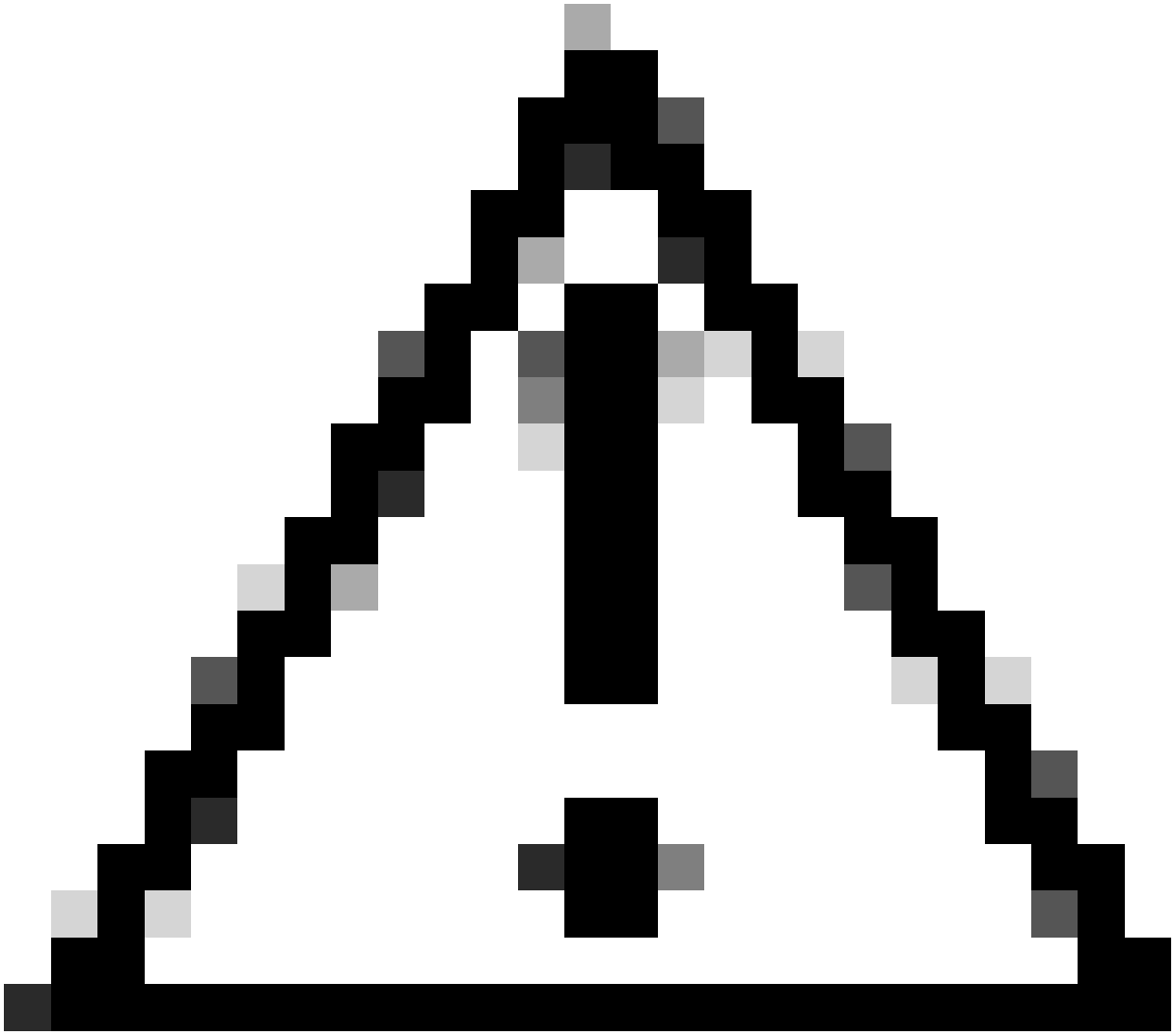



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

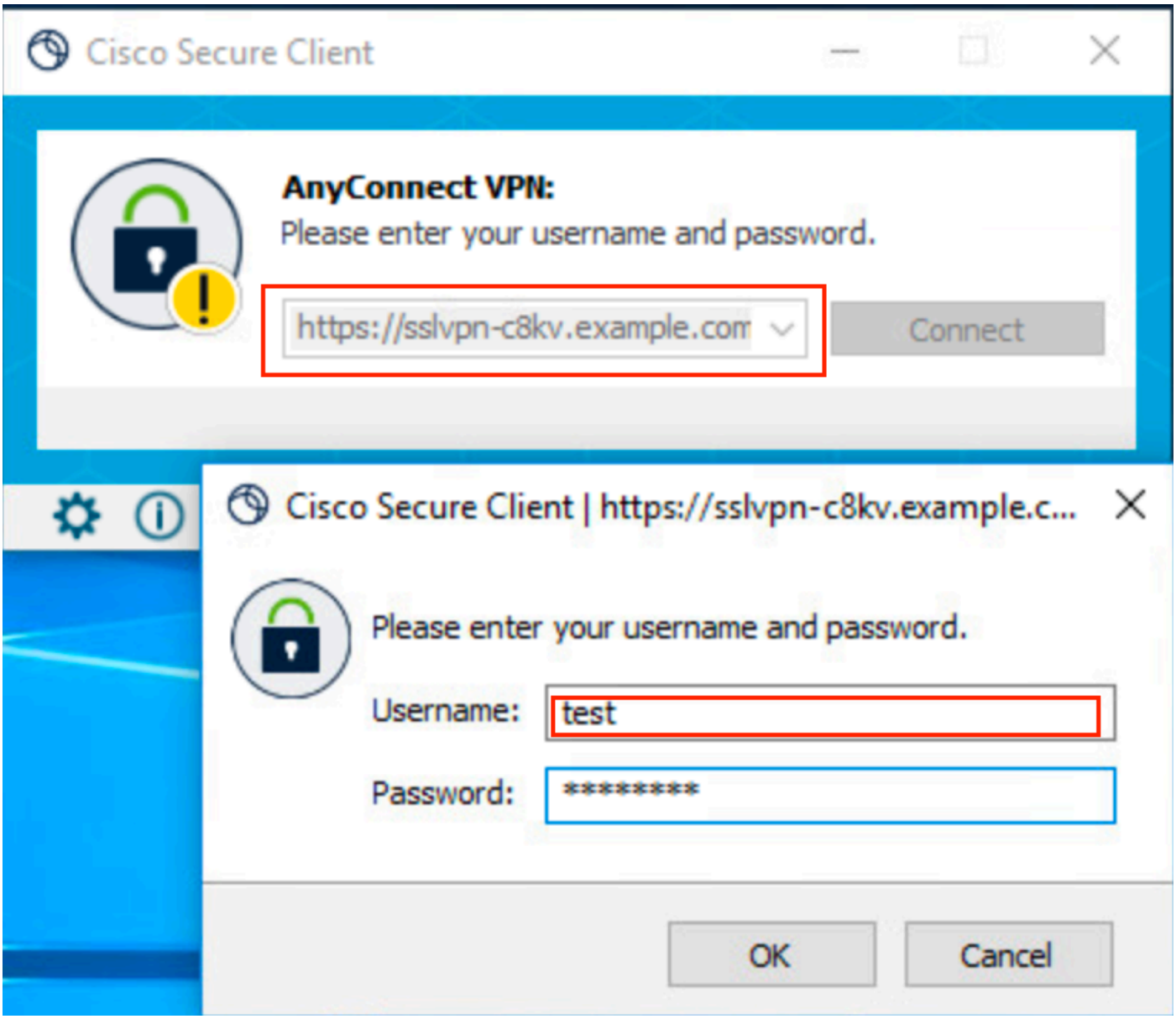
Flusso di connessione ad alto livello 2

Verifica

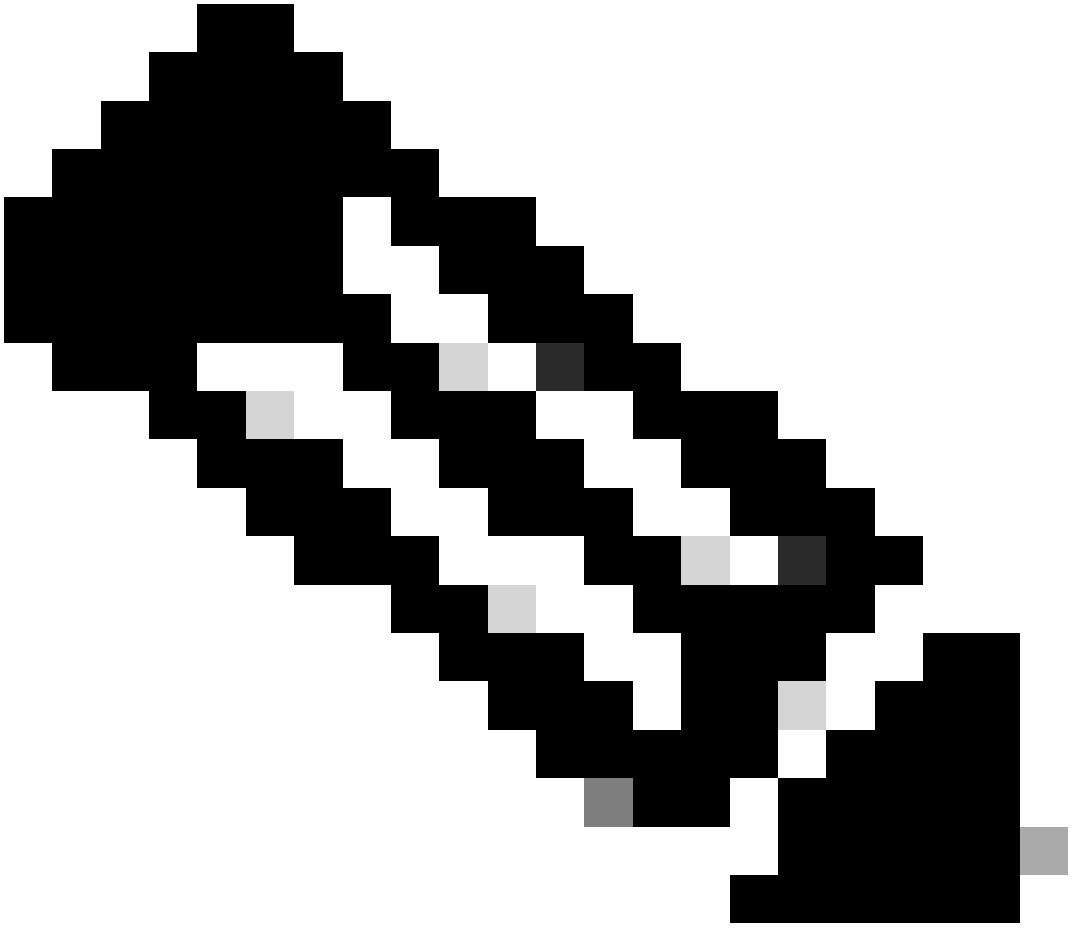
1. Per verificare l'autenticazione, connettersi da Cisco Secure Client con nome di dominio completo (FQDN) o indirizzo IP C800v e immettere le credenziali.



Attenzione: C800v non supporta il download di software client dall'headend. Cisco Secure Client deve essere preinstallato sul PC.



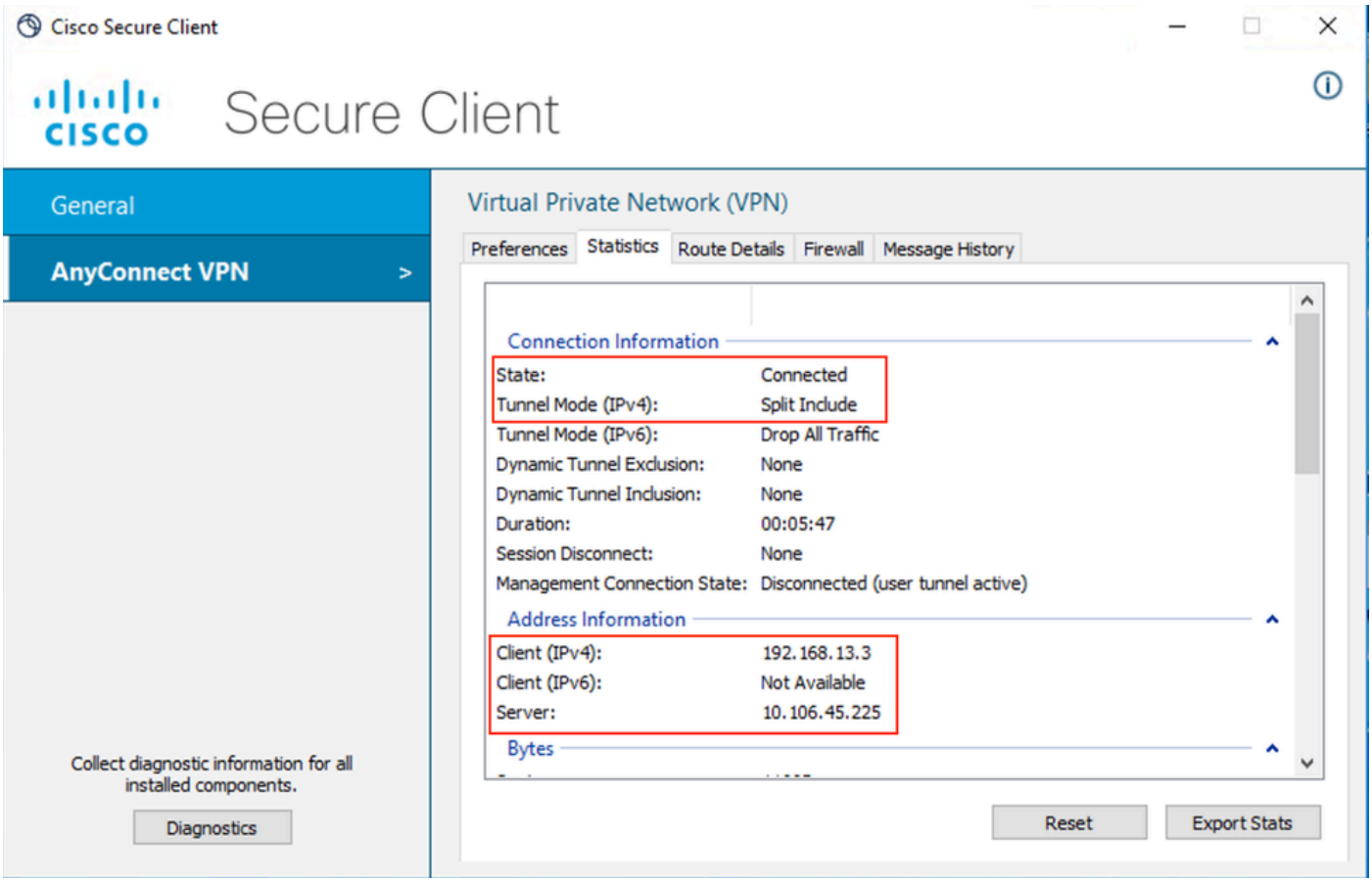
Tentativo di connessione di Cisco Secure Client



Nota: con una nuova installazione di Cisco Secure Client (senza profili XML aggiunti), l'utente può immettere manualmente il nome di dominio completo (FQDN) del gateway VPN nella barra degli indirizzi di Cisco Secure Client. Dopo aver eseguito correttamente l'accesso, Cisco Secure Client tenta di scaricare il profilo XML per impostazione predefinita. Tuttavia, per visualizzare il profilo nella GUI, è necessario riavviare Cisco Secure Client. La semplice chiusura della finestra di Cisco Secure Client non è sufficiente. Per riavviare il processo, fare clic con il pulsante destro del mouse sull'icona Cisco Secure Client nell'area di notifica di Windows e selezionare l'opzione Quit.

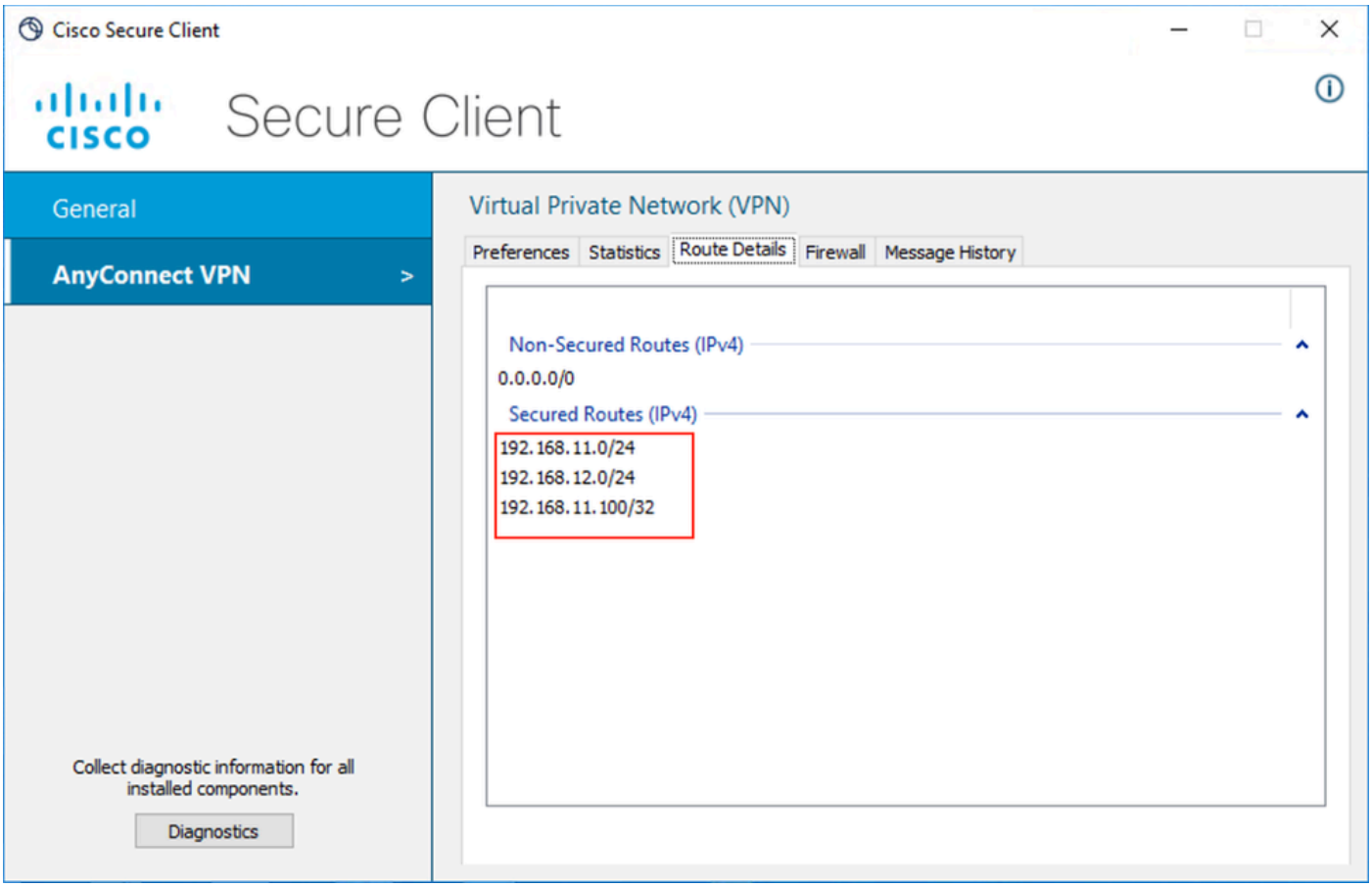
---

2. Una volta stabilita la connessione, fare clic sull'icona gear nell'angolo in basso a sinistra e selezionare AnyConnect VPN > Statistics. Verificare che le informazioni visualizzate corrispondano a Connection and Address Information.



Statistiche di Cisco Secure Client (AnyConnect)

3. Passare a AnyConnectVPN > Dettagli route e verificare che le informazioni visualizzate corrispondano alle route protette e non protette.



Dettagli sulla route di Cisco Secure Client (AnyConnect)

Per verificare che la configurazione funzioni correttamente su C800v, consultare questa sezione:

1. Per visualizzare le informazioni sulla sessione SSL - show crypto ssl session{user user-name |profile profile-name}

<#root>

sal_c8kv#show crypto ssl session user test

Interface :

Virtual-Access1

Session Type : Full Tunnel
Client User-Agent : AnyConnect Windows 5.1.8.105

Username : test Num Connection : 1
Public IP : 10.106.69.69
Profile :

ssl_prof

Policy :

ssl_policy

```
Last-Used : 00:41:40                    Created : *15:25:47.618 UTC Mon Mar 3 2025
Tunnel IP : 192.168.13.3                Netmask : 0.0.0.0
Rx IP Packets : 542                     Tx IP Packets : 410
```

sal_c8kv#show crypto ssl session profile ssl_prof

```
SSL profile name: ssl_prof
Client_Login_Name  Client_IP_Address No_of_Connections Created   Last_Used
cisco                10.106.69.69             1        00:49:41  00:49:41
```

2. Per visualizzare le statistiche sulla vpn ssl - show crypto ssl stats [profile name] [tunnel] [detail]

<#root>

sal_c8kv#show crypto ssl stats tunnel profile ssl_prof

```
SSLVPN Profile name : ssl_prof

Tunnel Statistics:

    Active connections       : 1
    Peak connections         : 1          Peak time               : 1d23h
    Connect succeed          : 13         Connect failed          : 0
    Reconnect succeed        : 0          Reconnect failed        : 0
    IP Addr Alloc Failed     : 0          VA creation failed      : 0
    DPD timeout              : 0

  Client

    in  CSTP frames          : 23         in  CSTP control        : 23
    in  CSTP data            : 0          in  CSTP bytes          : 872
    out CSTP frames          : 11         out CSTP control        : 11
    out CSTP data            : 0          out CSTP bytes          : 88
    cef in  CSTP data frames : 0          cef in  CSTP data bytes : 0
    cef out CSTP data frames : 0          cef out CSTP data bytes : 0

  Server

    In  IP pkts              : 0          In  IP bytes            : 0
    In  IP6 pkts             : 0          In  IP6 bytes           : 0
    Out IP pkts              : 0          Out IP bytes            : 0
    Out IP6 pkts             : 0          Out IP6 bytes           : 0
```

3. Controllare la configurazione effettiva applicata per l'interfaccia di accesso virtuale associata al client.

<#root>

sal_c8kv#show derived-config interface Virtual-Access1

```
Building configuration...

Derived configuration : 143 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context ssl_prof***
ip unnumbered GigabitEthernet1
ip mtu 1400
end
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

1. Debug del protocollo SSL per verificare la negoziazione tra l'headend e il client.

<#root>

debug crypto ssl condition client username

```
debug crypto ssl aaa
debug crypto ssl aggr-auth message
debug crypto ssl aggr-auth packets
debug crypto ssl tunnel errors
debug crypto ssl tunnel events
debug crypto ssl tunnel packets
debug crypto ssl package
```

2. Alcuni comandi aggiuntivi per verificare la configurazione SSL.

```
# show crypto ssl authorization policy
# show crypto ssl diagnose error
# show crypto ssl policy
# show crypto ssl profile
# show crypto ssl proposal
# show crypto ssl session profile <profile_name>
# show crypto ssl session user <username> detail
# show crypto ssl session user <username> platform detail
```

3. Strumento di diagnostica e segnalazione (DART) per Cisco Secure Client.
Per raccogliere il bundle DART, eseguire i passaggi descritti in Eseguire DART per raccogliere i dati per la risoluzione dei problemi

Debug di esempio di una connessione riuscita:

```
debug crypto ssl
debug crypto ssl tunnel events
debug crypto ssl tunnel errors
```

<#root>

```
*Mar 3 16:47:11.141: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:14.149: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891B8 total_len=621 bytes=621 tcb=0x0
*Mar 3 16:47:15.948: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: ssl_prof vw_gw: ssl_policy remote_ip: 10.106.
*Mar 3 16:47:15.948: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: LOCAL] [localport
*Mar 3 16:47:15.949: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=912 bytes=912 tcb=0x0
*Mar 3 16:47:17.698: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] CSTP Version recd , using 1
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-ERR]: IPv6 local addr pool not found
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] No free IPv6 available, disabling IPv6
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0]
SSLVPN reuqesting a VA creation
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Per Tunnel Vaccess cloning 2 request sent
*Mar 3 16:47:20.760: %SYS-5-CONFIG_P: Configured programmatically by process VTEMPLATE Background Mgr f
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[0] VACCESS: Received VACCESS PER TUNL EVENT response.
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Received vaccess Virtual-Access1 fro
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Cloning Per Tunnel Vaccess
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Interface Vi1 assigned to Session Us
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Allocating IP 192.168.13.4 from address-pool
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Using new allocated IP 192.168.13.4 0.0.0.0
*Mar 3 16:47:20.761: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 3 16:47:20.763: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Full Tunnel CONNECT request processed, HTTP r
*Mar 3 16:47:20.763: HTTP/1.1 200 OK
*Mar 3 16:47:20.763: Server: Cisco IOS SSLVPN
*Mar 3 16:47:20.763: X-CSTP-Version: 1
*Mar 3 16:47:20.763: X-CSTP-Address: 192.168.13.4
*Mar 3 16:47:20.763: X-CSTP-Netmask: 0.0.0.0
*Mar 3 16:47:20.763: X-CSTP-DNS: 192.168.11.100
*Mar 3 16:47:20.764: X-CSTP-Lease-Duration: 43200
*Mar 3 16:47:20.764: X-CSTP-MTU: 1406
*Mar 3 16:47:20.764: X-CSTP-Default-Domain: example.com
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.765: X-CSTP-Rekey-Time: 3600
*Mar 3 16:47:20.765: X-CSTP-Rekey-Method: new-tunnel
*Mar 3 16:47:20.765: X-CSTP-DPD: 300
*Mar 3 16:47:20.765: X-CSTP-Disconnected-Timeout: 0
*Mar 3 16:47:20.765: X-CSTP-Idle-Timeout: 1800
```

```
*Mar 3 16:47:20.765: X-CSTP-Session-Timeout: 43200
*Mar 3 16:47:20.765: X-CSTP-Keepalive: 30
*Mar 3 16:47:20.765: X-CSTP-Smartcard-Removal-Disconnect: false
*Mar 3 16:47:20.766: X-CSTP-Include-Local_LAN: false
*Mar 3 16:47:20.766: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] For User cisco, DPD timer started for 300 sec
*Mar 3 16:47:20.766: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=693 bytes=693 tcb=0x0
*Mar 3 16:47:21.762:
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).